REMARKS

The Applicants and the undersigned thank Examiner Colin for his careful and detailed review of this patent application. Claims 1-20 have been rejected. Upon entry of this amendment, Claims 1-15 and 17-20 will remain pending in this application.

The independent claims are Claims 1, 8, and 11. Consideration of the present application is respectfully requested in light of the above amendments to the claims, and in view of the following remarks.

Rejections under Obvious-Type Double Patenting

The Examiner provisionally rejected Claims 1, 8, 11, and 12 based on non-statutory obviousness-type double patenting as being unpatentable over claims 2-15 and 26-33 of copending Application Serial No. 09/607,375. The Applicants respectfully traverse this rejection.

In order to overcome this rejection, the Applicants have filed a terminal disclaimer incompliance with 37 C.F.R. § 1.321(c). Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Claim Rejections under 35 U.S.C. §103

The Examiner rejected Claims 1-20 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2001/0034847, published in the name of Stephen E. Gaul (hereinafter, the "Gaul reference") in view of U.S. Patent No. 6,438,600 issued in the name of Greenfield et al. (hereinafter the "Greenfield reference") and U.S. Patent No. 6,298,445 issued in the name of Shostack et al. (hereinafter the "Shostack reference").

The Applicants respectfully offer remarks to traverse these pending rejections. The Applicants will address each independent claim separately as the Applicants believe that each independent claim is separately patentable over the prior art of record.

Independent Claim 1

The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Gaul, Greenfield, and Shostack references fail to describe, teach, or suggest the

combination of: (1) issuing a request for a scanner from a browser operating on the workstation to a network server via a computer network; (2) transmitting the scanner from the network server to the workstation via the computer network, (3) the scanner installable within the browser and operative to complete a vulnerability assessment of the workstation (4) to identify security vulnerabilities of the workstation that can (5) compromise secure operation of the workstation on the computer network; (6) generating workstation credentials derived from the scanner conducting the vulnerability assessment of the workstation, (7) the workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation; (8) comparing the workstation credentials to a workstation policy; (9) authenticating a workstation for access to the network server after authenticating the workstation by (10) granting the workstation access to one or more services available on the network server if (11) the workstation credentials derived from the scanner are in compliance with the workstation policy; (12) if access to the one or more services available on the network server is granted to the workstation because the workstation credentials are in compliance with the workstation policy, issuing a request for credentials associated with a user; (13) receiving credentials associated with a user; and (14) authenticating a user of the workstation for access to the network server (15) after authenticating the workstation for access to the network server (16) by determining if the user is authorized to access the one or more services available on the network server (17) through evaluating the credentials associated with the user, as recited in amended independent Claim 1.

The Gaul Reference

The Gaul reference describes a system that allows Systems Administrators and Network Managers to perform Internet security vulnerability assessments from outside of an organization's firewall 37. See Gaul reference, page 2, first column, paragraph 0016. The system of the Gaul reference allows a system administrator to use an internet browser running on a client 36 to access an external Internet-based Network Security Vulnerability Testing (NSVT) application 41 and an internal Network Security Vulnerability Testing (NSVT) application 38. See Figure 1 of the Gaul reference reproduced below.

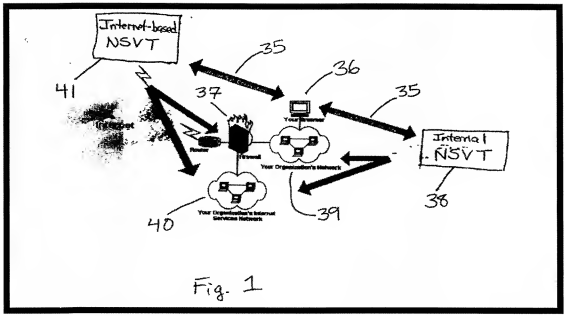

Fig. 1

With NSVT applications 38, 41 the user running the client 36 can launch security testing against any one system or multiple systems. See Figure 1 of the Gaul reference reproduced above and page 3, first column, paragraph 0031.

The Gaul reference provides security testing or vulnerability testing of its computer system elements, but it does not use its security testing or vulnerability testing in connection with allowing a computer system element to gain access to a network or service. The Gaul reference is only concerned with random testing of its system components under control of system administrators and repairing those components if the components fail a test.

Meanwhile, the Applicants' invention generates workstation credentials that are derived from a scanner conducting a vulnerability assessment of the workstation; compares the workstation credentials to a workstation policy; the invention authenticates a workstation for access to the network server after authenticating the workstation by granting the workstation access to the network server if the workstation credentials derived from the scanner are in compliance with the workstation policy; if access to the network server for the workstation is granted because the workstation credentials are in compliance with the workstation policy, a request is issued for credentials associated with a user in order to authenticate a user of the workstation for access to the network server

after authenticating the workstation for access to the network server by determining if the user is authorized to access the one or more services available on the network server, as recited in amended independent Claim 1.

The Greenfield Reference

The Greenfield reference generally describes a computer program for securely sharing log-in credentials among trusted browser-based applications. Credentials for a user can be automatically shared only among a restricted and authorized set of trusted applications, without requiring the application developer to write code to manage the credentials. A single log-in is used to obtain the user credentials for a particular codebase, and the credentials are then reused for applications in that codebase. See Greenfield reference, Abstract.

The Examiner alleges that Figure 3 of the Greenfield reference teaches the transmitting of workstation credentials to a server. The Greenfield reference explains Figure 3 illustrates one approach that may be used to verify credentials, and involves transmitting the credentials to a server.

Block 325 in Figure 3 sends the credentials and the command (i.e. the request for a secured operation) to a server. This information is received by the server at Block 330, and verified (using application-specific processing, as previously stated) at Block 335. A test is made at Block 340 to determine whether the result of the verification process indicates that the user is authorized. If so, Block 345 performs the requested command, and Block 355 returns the result to the client machine. The applet then continues its execution, using these returned results, at Block 360. See Figure 3 of the Greenfield, reproduced below and column 8, lines 26-38.

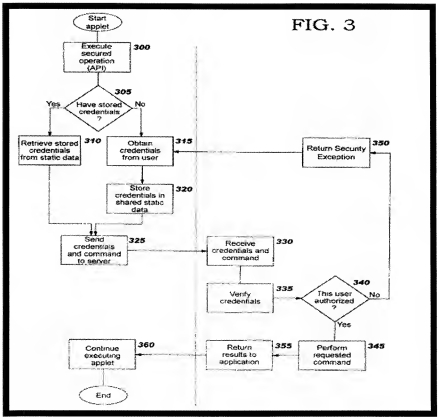

FIG. 3

While the Greenfield reference may teach transmitting "credentials" from a workstation to a server, these are credentials that are associated with a user and not ones derived from a scanner conducting a vulnerability assessment of the workstation. The Greenfield "credentials" are not workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation, as recited in amended independent Claim 1.

The Greenfield reference defines credentials as application-specific information (such as a user name or other identifier, a user password, etc.) that identifies the requesting user at the client machine. These credentials are compared to a previously-defined, stored set of the credentials for all authorized users. If the credentials match an entry in this stored set, then this user is an authorized user. See Greenfield reference, column 2, lines 48-55. Therefore, while the Greenfield reference teaches authenticating a user, the Greenfield reference does not teach granting a workstation access to a service prior to authenticating a user to access the service.

The Shostack Reference

The Examiner admits that the Gaul and Greenfield references fail to provide any teaching of granting a workstation access to one or more services available on a network server if the workstation credentials are in compliance with the workstation policy, prior to granting a user access to one or more services available on a network server. To make up for this critical deficiency, the Examiner relies upon the Shostack reference to provide such a teaching.

The Shostack reference describes a system that automatically provides, in real-time, software enhancements with-updated information regarding security vulnerabilities. A user, system administrator, server, etc. is able to implement prevention techniques before a security breach occurs. With the system of the Shostack reference, the enhancement that was sent is then integrated into the computer security software. Before the integration, a computer check can be performed to determine the integrity and the authenticity of the enhancement. The computer check can use cryptographic techniques such as digital signatures and Pretty Good Privacy (PGP) encryption. Shostack reference, column 2, lines 30-48.

The integrated system 160 of the Shostack reference includes a database 92 of security vulnerabilities that provides a secure operating environment. A first module 74 accesses the database 92 and assesses security vulnerabilities of an operating system of a computer. A second module 76 accesses the database and assesses security vulnerabilities of a computer network that includes the computer. A third module 78 accesses the database and assesses security vulnerabilities in passwords used to access the computer or the network. A fourth module 88 accesses the database and assesses security vulnerabilities of a remote computer connected to the network. A fifth module 90 receives an update to the database and updates the database. A sixth module is a communications module that allows communication between the integrated security system and a similar system. See Figure 5 below that illustrates the aforementioned modules of the integrated system 160. Shostack reference, column 11, line 61 through column 12, line 14.

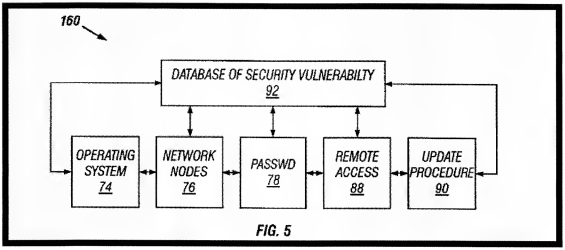

FIG. 5

The Shostack reference explains that the aforementioned and above illustrated modules 74-90 of the integrated system 160 are represented by corresponding symbols on a graphical user interface (GUI) screen 70 that is illustrated in Figure 6 below.

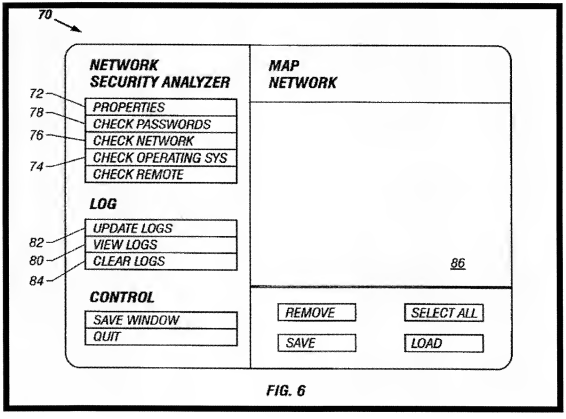

FIG. 6

The Shostack reference explains that the GUI 70 as illustrated in Figure 6 above provides a reporting mechanism. The GUI 70 includes several means for reporting various network transactions. The GUI 70 includes a log view 80 that may allow a user to view a text version of an update process or log information on a storage device, a log update 82 that generates a report of all security vulnerabilities on the network 20, and a log clear function 84 that allows a user to erase the log. Shostack reference, column 13, lines 37-44.

As noted above, the Examiner relies upon the Shostack reference to provide an alleged teaching of using a network security detector to scan the network for violators and assessing vulnerabilities of a remote computer before permitting a user access to a networks. However, the Shostack reference is simply not a gatekeeper or server that controls access to a computer network by first granting access to a computer and then, second, access to a user of the computer, as alleged by the Examiner. Instead, the Shostack reference is a vulnerability testing tool for monitoring new software updates and installations and that may check a status of a current connection.

Fourth Module of Shostack Reference: Testing Services Accessed by a Remote Computer

The Shostack reference describes how the fourth module 88 of the system 160 accesses the database of security vulnerabilities 92 and assess the security vulnerabilities of a remote computer connected to the network. The fourth module 88 allows a remote computer to first connect to a network service and then accepts information from the service and like the second module 76, it also interrogates the service. Shostack reference, column 13, lines 1-6. The fourth module 88 is not designed to operate as a gatekeeper as this description indicates. But instead, the fourth module 88 only tests or "interrogates" the service that can be accessed by the remote computer. The fourth module 88 also does not grant a user access to a network.

Fifth Module of Shostack Reference: Checks Authenticity of Software Updates

The fifth module 90 of the Shostack reference is for receiving an update to the database of security vulnerabilities 92 and updating the database. The fifth module 90 includes the installer 58. The fifth module 90 checks the authenticity and integrity of the

software enhancement. The authenticity of the software enhancement works for either an update or a new version. The authenticity and integrity of the software enhancement is confirmed using cryptographic methods with PGP output from the network security detector 16. In one aspect of the Shostack reference, the fifth module 90 also maintains a record of all transactions. Shostack reference, column 13, lines 10-17.

Sixth Module of Shostack Reference: Constantly Checks User Identification

A sixth module of the Shostack reference is a communications module that allows the integrated security system 160 to communicate with a similar system over a computer network. The sixth module may allow communication between the similar system and the various modules and software applications for sharing database files, for sharing workload in breaking long lists of passwords, transmitting reports or data for purposes of analysis, reporting to a management station, configuring files or configuring an operating system, and invoking a remote system to send a software enhancement. The sixth module may also include cryptographic code for protecting the confidentiality and integrity of the information being transmitted. Shostack reference, column 13, lines 18-29.

The sixth module may be used for authenticating a user and providing a means for reporting various transactions on the network 20. Specifically, the sixth module may be used to constantly check a user's identification, the integrity of the service connection, and the status of any network processing. Shostack reference, column 13, lines 30-36.

Summary for Independent Claim 1

The prior art of record does not provide any teaching of generating workstation credentials derived from a scanner conducting the vulnerability assessment of the workstation and where the workstation credentials comprise at least one of information about integrity of the workstation and a security posture of the workstation. The prior art does not provide any teaching of comparing the workstation credentials to a workstation policy in order to grant the workstation access to one or more services available on a network server if the workstation credentials are in compliance with the workstation policy, prior to granting a user access to one or more services available on a network server.

To emphasize that the prior art of record does not grant access to a network service for a workstation, but instead, only authenticates a user to access a service, the amended independent claims recite that a request for credentials associated with a user is issued after a workstation is granted access to a service in order to determine if the user is authorized to access the a service available on a network server. This means that each of the independent claims require at least two authentication steps: (1) granting a physical workstation access to a service; and then (2) granting a user access to a service if the physical workstation is granted access to the service.

In light of the differences between amended independent Claim 1 and the Gaul, Greenfield, and Shostack references noted above, one of ordinary skill in the art recognizes that these prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of the rejection of Claim 1 are respectfully requested.

Independent Claim 8

The rejection of Claim 8 is respectfully traversed. It is respectfully submitted that the Gaul, Greenfield, and Shostack references, fail to describe, teach, or suggest the combination of: (1) issuing a request for a scanner to a network server from a browser operating on the workstation; (2) transmitting the scanner and (3) a workstation policy from the network server to the workstation via the computer network, (4) the scanner installable within the browser and (5) operative to generate workstation credentials by (6) completing a vulnerability assessment of the workstation, the workstation credentials comprising (7) at least one of information about integrity of the workstation and a security posture of the workstation; (8) comparing the workstation credentials to the workstation policy on the workstation (9) to determine whether the workstation should be granted access to the software service; (10) authenticating a workstation for access to the software service after authenticating the workstation by (11) granting the workstation access to the software service available on the network server (12) if the workstation credentials (13) derived from the scanner are in compliance with the workstation policy; and (14) if access to the software service is granted to the workstation because the workstation credentials are in compliance with the workstation policy, (15) authenticating

a user of the workstation for access to the software service (16) after authenticating the workstation for access to the software service by (17) issuing a request for user authentication in order to (18) determine if a user of the workstation is authorized to access the software service available on the network server, as recited in amended independent Claim 8.

As noted above with respect to independent Claim 1, the Gaul, Greenfield, and Shostack references do not provide any teaching of granting access to a system or network for a workstation and then requesting further information about a user of the workstation in order to authenticate a user when the workstation has been granted access to the network.

In light of the differences between Claim 8 and the references mentioned above, one of ordinary skill in the art recognizes that the Gaul, Johnson, and Shostack references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in independent Claim 8. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 11

The rejection of Claim 11 is respectfully traversed. It is respectfully submitted that the Gaul, Greenfield, and Shostack references, fail to describe, teach, or suggest the combination of: (1) issuing a request for a scanner to the network server (2) from a browser operating on the workstation; (3) transmitting the scanner from the network server to the workstation via the computer network, (4) the scanner installable within the browser and operative to (5) generate workstation credentials by (6) completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network, (7) the workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation; (8) transmitting the workstation security credentials from the scanner to the network server via the computer network; (9) determining at the network server whether the workstation should be granted access to a network service of the network based on the workstation credentials; and (10) authenticating a workstation for access to the network service after authenticating the

workstation by (11) granting the workstation access to the network service if the workstation credentials (12) derived from the scanner are in compliance with the workstation policy; and (13) if access is granted to the workstation for the network service because the workstation credentials are in compliance with the workstation policy, (14) authenticating a user of the workstation for access to the network service (15) after authenticating the workstation for access to the network service by (16) issuing a request for information relating to user authentication in order to (17) determine if the user is authorized to access the network service, as recited in amended independent Claim 11.

In light of the differences between amended Claim 11 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 11. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Dependent Claims 2-7, 9-10, and 12-15, and 17-20

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited references.

The Applicants also respectfully submit that the recitations of all the dependent claims are of patentable significance. Accordingly, reconsideration and withdrawal of the rejections of the dependent claims are respectfully requested.

CONCLUSION

The foregoing is submitted as a full and complete response to the Office Action mailed on January 24, 2006. The Applicants and the undersigned thank Examiner Colin for the consideration of these remarks. The Applicants have submitted remarks to traverse the rejections of Claims 1-15 and 17-20. The Applicants respectfully submit that the present application is in condition for allowance. Such Action is hereby courteously solicited.

If any issues remain that may be resolved by telephone, the Examiner is requested to call the undersigned at 404.572.2884.

Respectfully submitted,

/SPW/

Steven P. Wigmore
Reg. No. 40,447

July 24, 2006

King & Spalding LLP
34th Floor
1180 Peachtree St. NE.
Atlanta, Georgia 30309
404.572.4600
K&S Docket: 05456-105007